Proposal of Hazard Analysis Method extending STPA using State Transition Diagram

Dai Funayama, Youichi Tomioka, and Junji Kitamichi
The University of Aizu, JAPAN

Index

1. Background of research
2. Our solution of the problem
3. Proposed method
4. GUI tool supporting proposed method
5. Evaluation
6. Conclusion

Background of this research

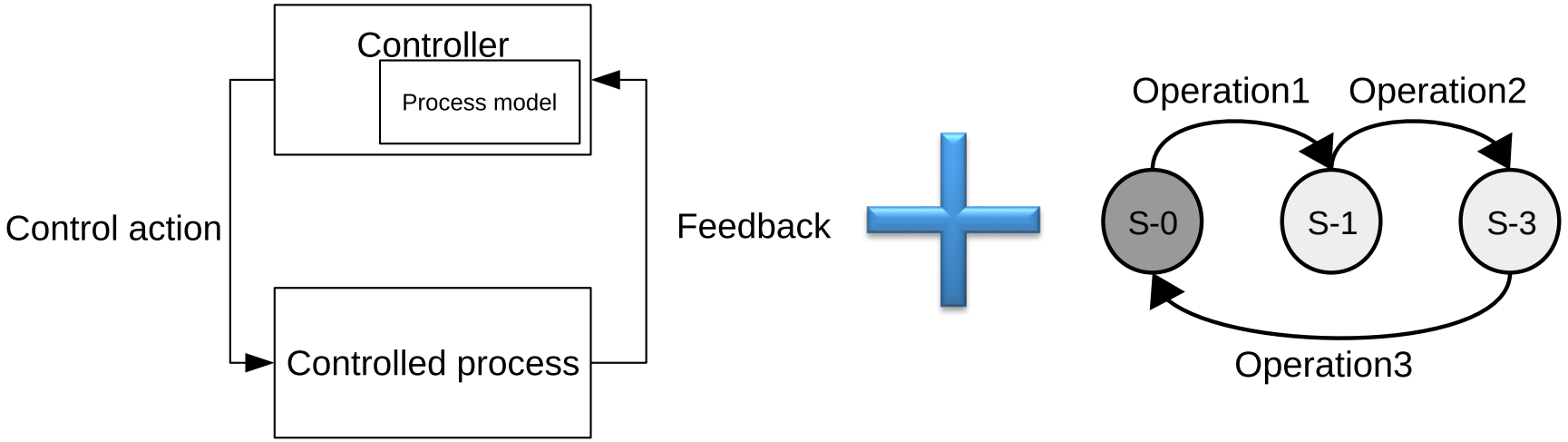
- We can apply STAMP/STPA to systems with complicated structures.
- In the analysis of such systems, it is difficult to extract accidents comprehensively.

Problem:
Examples of accidents which are difficult to extract

- Accidents caused by state and transition deviations
- Accidents caused by consecutive operations
- Accidents caused by unspecified parts in a system design

Our solution for the problem

- Adding concept of a state transition diagram to STAMP for more comprehensive analysis
- Enable extraction of accidents related to states and transitions



Proposed method

We propose a new analysis method based on STPA.

The unique points of the proposed method are as follows:

- Design of a new analysis model using a state transition diagram
- Definition of new guide words refer to existing analysis methods
- Use of a state transition diagram for extract Unsafe Control Action (UCA) comprehensively

Existing analysis method using state transition diagram

- Adding concept of a state transition diagram refer to **SASTD** (Safety Analysis method base on State Transition Diagram)
- SASTD analyzes a system based on state transition diagram and extracts deviations
- SASTD uses 8 guide words for extract state and transition deviations

Example of guide words

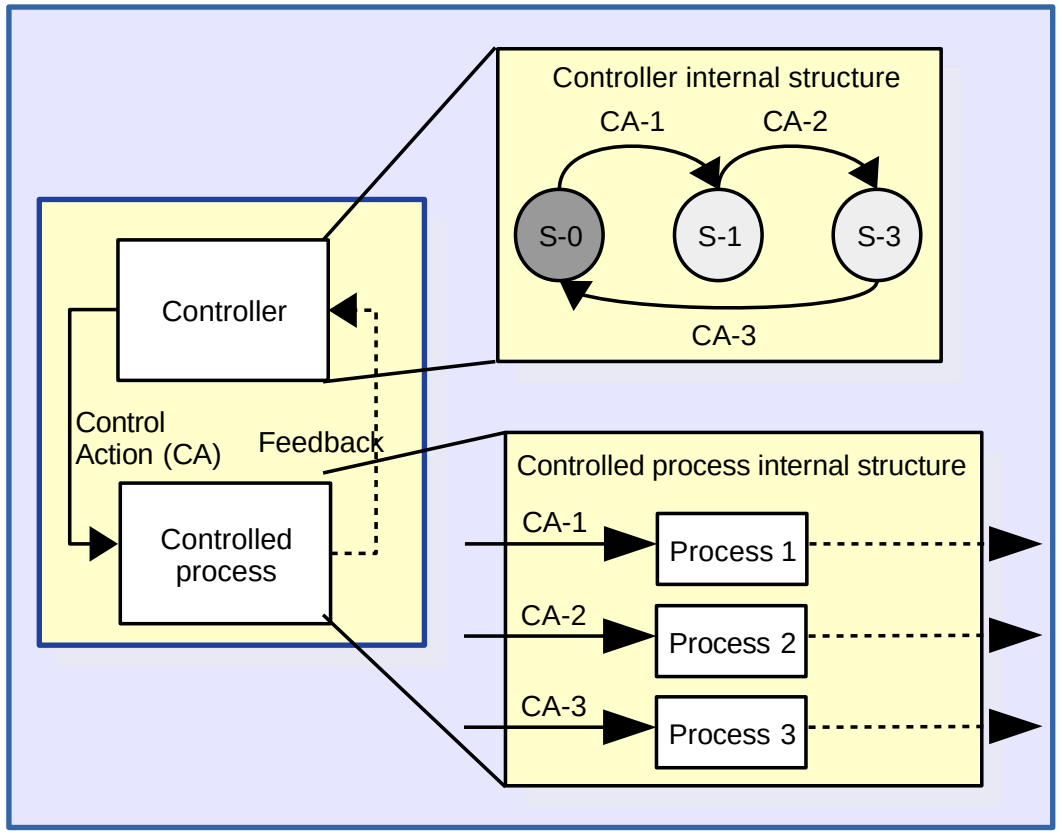
<u>Deviation-related states:</u>

- Transition occurs even though no event has occurred

<u>Deviation-related transitions:</u>

- Transition to the wrong state occurs, and unnecessary actions are executed
- Transition occurs earlier or later than the assumed timing, and necessary actions are executed

Proposed analysis model



- STAMP model with internal structure
- Controller is a state transition diagram showing its behavior
  - States: Current state of the controlled process
  - Transitions: Control actions of the controller
- Controlled process contains classes that receives control action and executes corresponding process

Analysis process using proposed method

- The analysis process in the proposed method is basically similar to STPA
- The process of designing state transition diagram of the controller is added
- The process of extracting UCA is modified to confirm to the proposed method

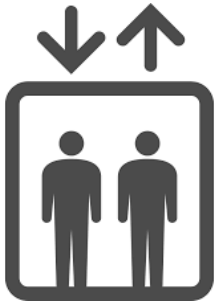
Analysis process

1. Extraction of accidents, hazards, and safety constraints
2. Design of control structure
3. Design of state transition diagram of the controller
4. Extraction of UCAs using state transition diagram
5. Identification of Hazard Causal Factors (HCFs)

In this time, we explain about process 3 and 4 in detail.

Design of state transition diagram of the controller

Example: Elevator door control system

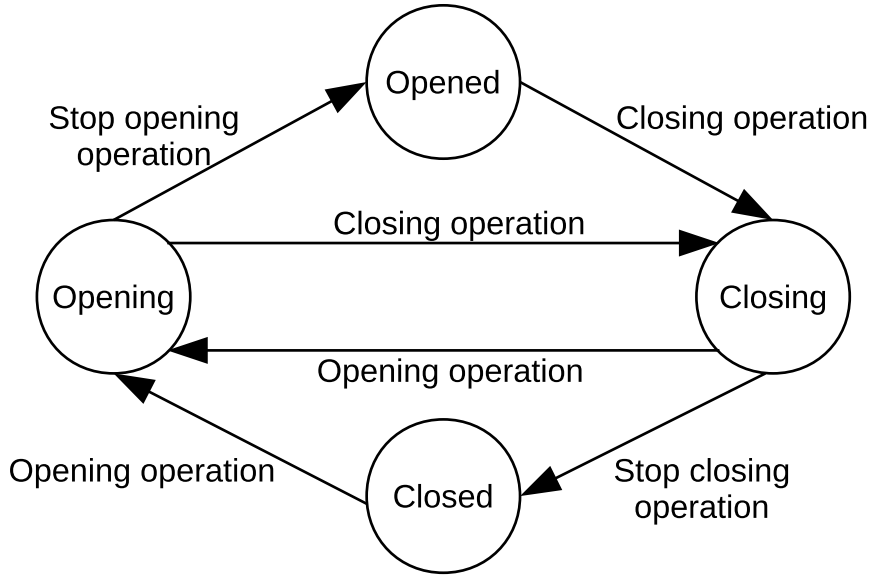


Controlled process has 4 states :

“Closed”, “Opening”, “Opened”, and “Closing”

Controller has 4 control actions:

“Opening operation”, “Stop opening operation”, “Closing operation”, and “Stop closing operation”



Elevator door control system

Definition of guide words

- Definition of new guide words for use in extracting UCA in proposed method
- Guide words are defined so that it can cover the entire analysis area of guide words in STPA and SASTD

Newly defined guide words

- Incorrect transition
- No transition
- Transition occurs, but some necessary actions are not executed
- Transition occurs, but some unnecessary actions are executed
- Too early/late transition
- Incorrect parameters in the process model

Extraction of UCAs using state transition diagram

State	CA	UCAs					
		1. Incorrect transition	2. No transition	3. Some necessary actions are not executed	4. Some unnecessary actions are executed	5. Too early / late transition	6. Incorrect parameters of the process model
Closed	Opening					UCA1. The door opens before the elevator comes	
	Stop Opening						
	Closing						
	Stop Closing						
Closing	Opening					UCA1. The door opens before the elevator comes	
	Stop Opening						
	Closing			UCA2. The elevator moves without the door closing			
	Stop Closing						

UCA2. The elevator moves without the door closing

- Extraction of UCAs for each states and transitions
- It is enable to exclude dark blocks because these part cannot be the cause of UCA

GUI tool supporting proposed method

- Development of a GUI tool supporting analysis using the proposed method
- Referring to existing analysis tools, XSTAMPP, STAMP Workbench and others

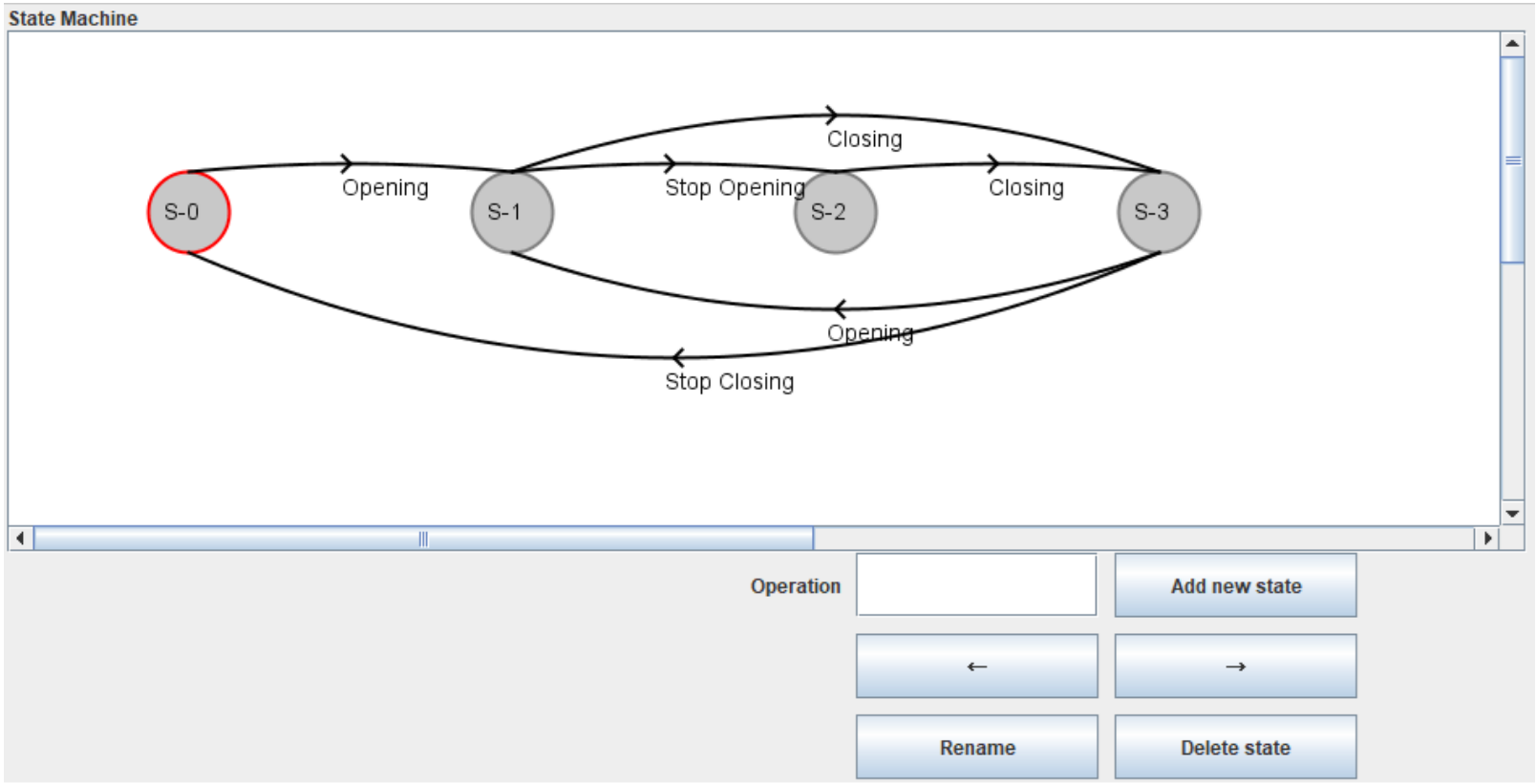
Functions of developed tool:

1. Extraction and linking of accidents, hazards, and safety constraints
2. Design of control structure
3. Design of state transition diagram
4. Extraction of UCAs using state transition diagram
5. Identification of HCFs

GUI tool – State transition diagram view

The possible operations on this view are as follows:

- Design of state transition diagram with GUI
- Editing states and transitions freely
- Assignment of control action for each transition

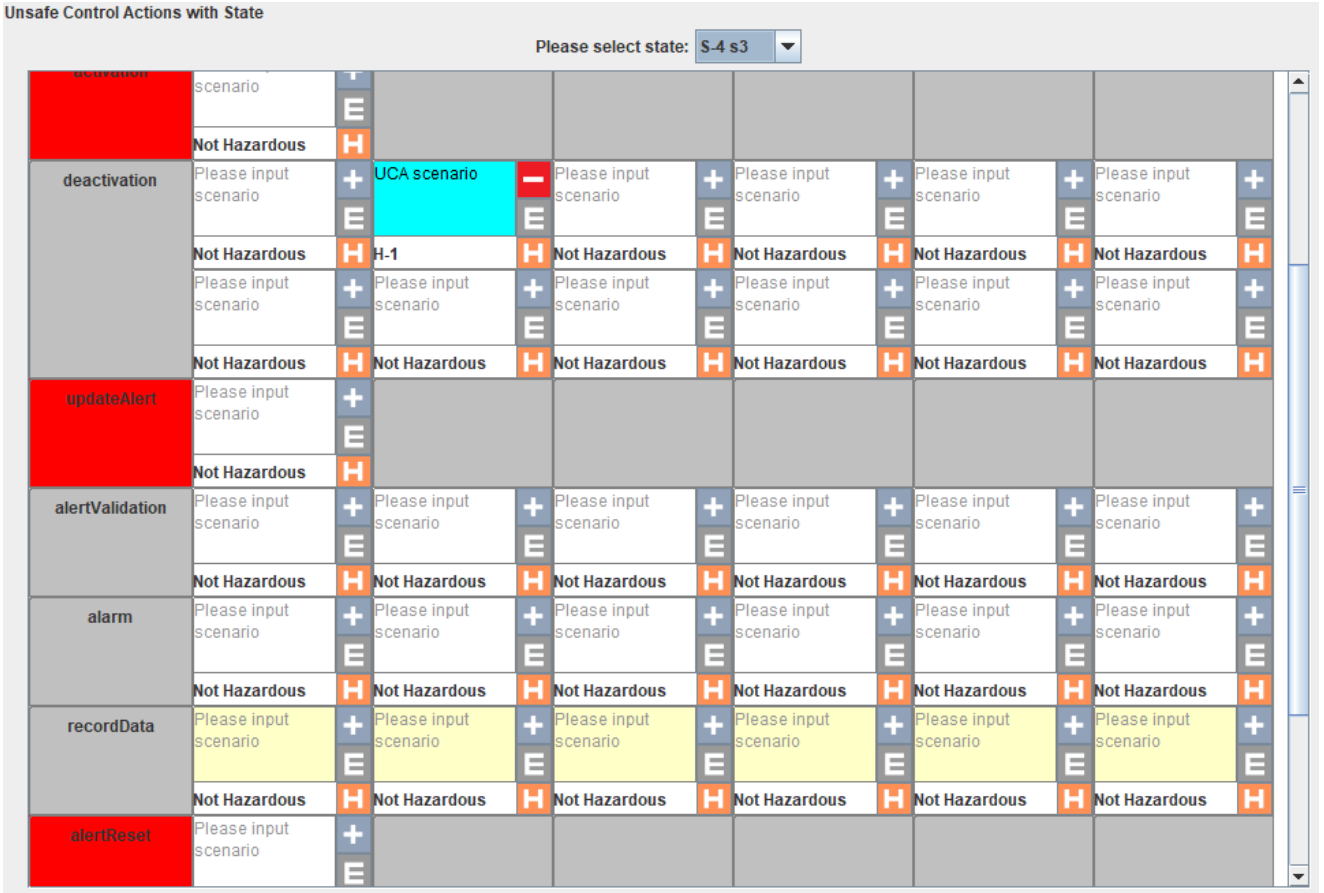


State transition diagram view

GUI tool – Extracting UCA table view

The possible operations on this view are as follows:

- Analysis and registration of UCA scenario with 6 guide words
- Excluding parts that do not require analysis automatically
- Picking up blocks that are likely to lead to UCA



Extracting UCA table view

Evaluation

- Applying the proposed method to a target system
- Evaluation of the proposed method and the developed tool

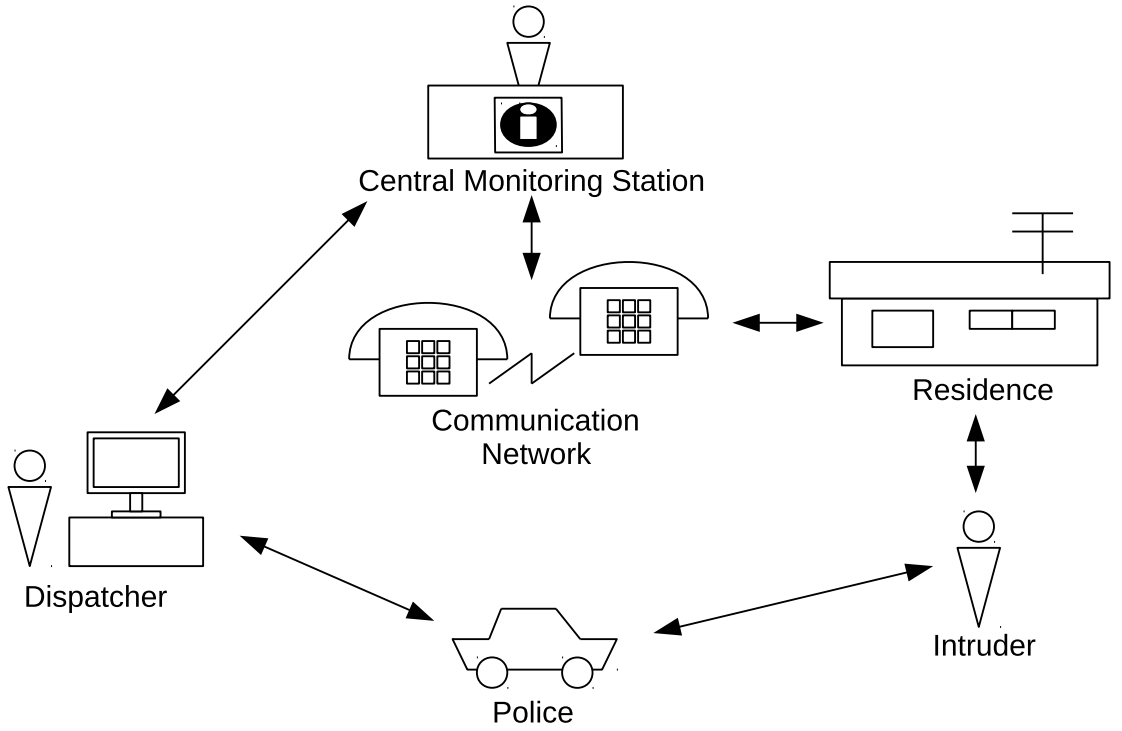
Evaluation criteria:

- Ease of extraction of UCA
- Performance to extract hazard

Evaluation - Target system

Residential Security system[1]

- It is a security system consists of multiple components.
- Security system senses an intruder, the central monitoring station observer reports the police and dispatches police officers to the residence.



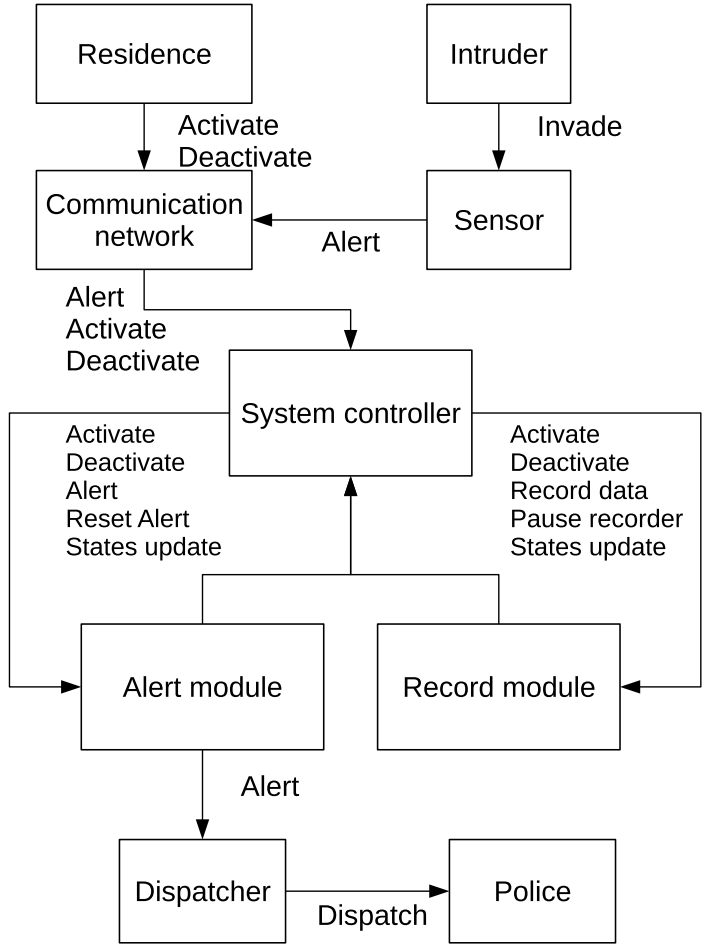
Residential Security system

[1]A Practical Guide to SysML SECOND EDITION

Evaluation - Analysis data

Accidents	Hazards	Safety constraints
An Intruder is not notified and contacts with a resident	The system does not notify an intruder	The system must notify when sensing intruders
A resident is notified as intruders	The system notifies a resident as intruders	The system must not notify while a resident set to deactivate

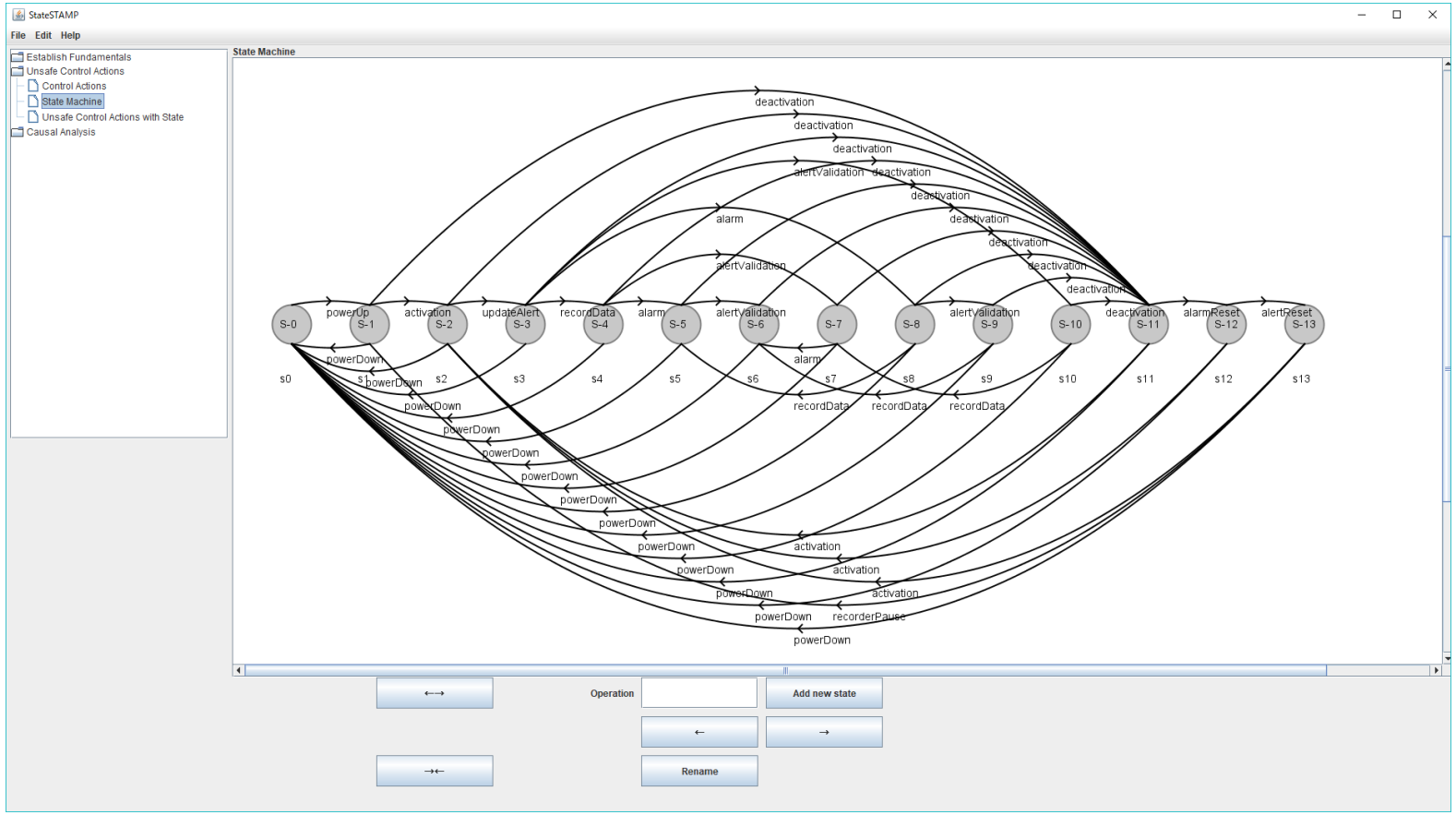
List of accidents, hazards, and safety constraints



Control structure

Evaluation – Design of a state transition diagram

- Using developed tool to design a state transition diagram
- The controller of the target system is represented by parallel state transition diagram, and it is synthesized to a flat diagram (product machine)
- Target system has complicated structure
  - 13 states
  - 33 transitions
  - 11 kinds of CA



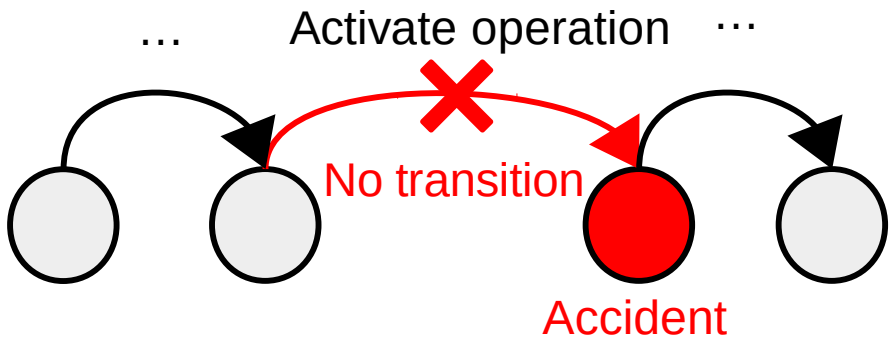
Designed state transition diagram

Evaluation - Result

We can extract UCAs easily by using concept of state transition diagram.
Number of extracted UCAs : 10

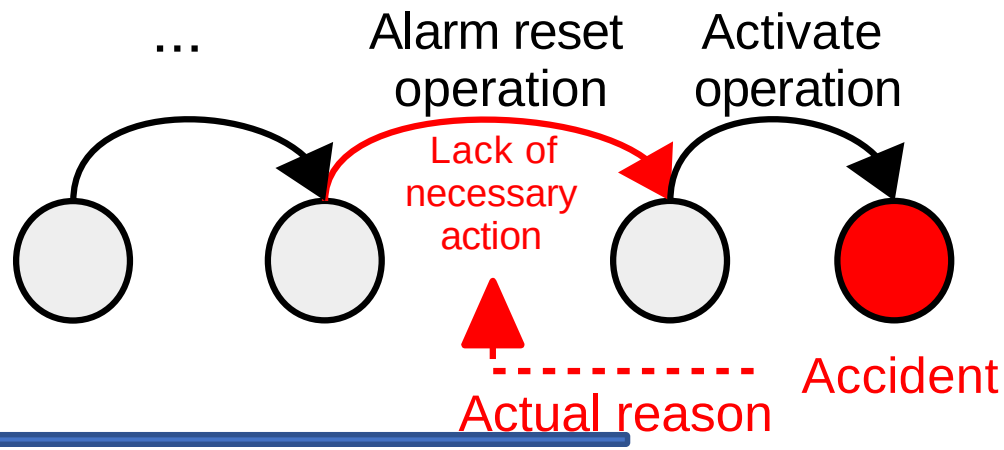
- UCA caused by lack of transition

Example. System does not give activate operation and an Intruder contacts with a resident.



- UCA caused by consecutive operations

Example. An Alarm is activated without reset and does not ring properly because of the lack of reset operation.



Conclusion

- We can extract UCAs easily and comprehensively with the proposed method.
  - Specifying unspecified states and transitions that are not directly connected to UCA.
  - Tracing the process to UCA easily because the system is expressed by the state transition diagram.
- We can analyze complicated systems efficiently by using the developed tool.